FortiAuthenticator - Release Notes

Version 6.0.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

2019-03-14
FortiAuthenticator 6.0.0 Release Notes
23-600-543486-20190314

TABLE OF CONTENTS

Change log

Date	Change Description
2019-03-14	Initial release.
2019-03-20	Updated Upgrade instructions on page 11 to include workaround for upgrading from FortiAuthenticator 5.3.1.

FortiAuthenticator 6.0.0 Release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.0.0, build 0010.

FortiAuthenticator is a user and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, and Fortinet Single Sign-On (FSSO).

For additional documentation, please visit:

https://docs.fortinet.com/product/fortiauthenticator/

Special notices

TFTP boot process

The TFTP boot process erases all current FortiAuthenticator configuration and replaces it with the factory default settings.

Monitor settings for web-based manager access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the web-based manager to be viewed properly without need for scrolling.

Before any upgrade

Save a copy of your FortiAuthenticator unit configuration prior to upgrading. Go to **System > Dashboard > Status** and select **Backup/Restore > Download backup file** to backup the configuration.

After any upgrade

If you are using the web-based manager, clear your browser cache prior to login on the FortiAuthenticator to ensure the web-based manager screens are displayed properly.

What's new

FortiAuthenticator version 6.0.0 includes the following new features and enhancements:

GUI update

The FortiAuthenticator GUI has been updated to match the look and feel of FortiOS 6.0.

SAML IdP proxy for cloud identity services

FortiAuthenticator can be configured to act as a SAML Identity Provider (IdP) proxy for cloud identity services, such as G Suite and Azure. The cloud identity service is used as the SAML IdP for authentication and its OAuth/API service for group lookups. This enables the SAML IdP service on FortiAuthenticator to add a two-factor authentication service by acting as an IdP proxy.

Improvements to remote LDAP user synchronization rules

When configuring a remote LDAP user synchronization rule, new options enable you to:

- Specify which user role (User, Sponsor, Administrator) to assign to imported users. Users assigned the role of Administrator are granted full permissions.
- Delete all users when an LDAP query result is empty.

OAuth server capability

FortiAuthenticator can act as an authorization server to issue and manage OAuth access tokens via a set of REST API endpoints. An OAuth client is issued an OAuth access token by FortiAuthenticator after successfully providing its login credentials. The OAuth client can then use this access token as proof of authorization to access a third-party service. The third-party service may contact FortiAuthenticator to validate any given OAuth access token.

Use FortiNAC as sources of SSO sessions

FortiAuthenticator can retrieve SSO sessions from FortiNAC servers and use these sessions as a new FSSO source for relay to FortiGate devices. From the SSO Configuration page (*Fortinet SSO Methods* > *SSO* > *General*), you can:

- Enable FortiNAC SSO.
- Configure FortiNAC sources.
- Select one or more FortiNAC sources to use as FSSO sources.

FSSO domain monitor improvements

The SSO domain monitor includes the following improvements:

- The status of all configured domain controllers is displayed, even ones not reachable during domain exploration. Each domain controller is displayed in:
  - green if the last connection attempt was successful
  - gray if no recent connection information is available
  - red if the last connection attempt failed
- View recent connection activity for each domain controller.
- View debug logs generated when performing the domain manager's domain structure discovery.
- Rebuild the domain structure.

HTTPS/HTTP access controls

More granular HTTPS/HTTP access controls allow you to enable or disable HTTPS/HTTP access for each service on a selected network interface.

Enhanced cryptography for local user password storage

FortiAuthenticator offers the option to use stronger cryptography for the storage of local user passwords, available under General Account Policy Settings (*Authentication* > *User Account Policies* > *General*).

This option cannot be disabled after 30 days of being enabled. FortiAuthenticator will send an email reminder to the administrator before the end of the 30-day period.

Configurable error pages

The content of error pages can be customized to provide more helpful messages to users. The following error messages are configured on the Replacement Messages page (*Authentication* > *Self-service Portal* > *Replacement Messages*):

- 500 Internal Server Error
- 503 Service Unavailable Error
- 404 Not Found
- 403 Forbidden

FortiOS Security Fabric integration

FortiAuthenticator supports integration with the Fortinet Security Fabric. Starting in FortiOS 6.2, you can add the following FortiAuthenticator widgets to the FortiOS dashboard:

- System Information
- User Inventory

- Authentication Activity
- Top User Lookouts

G Suite and Azure group lookup for SAML SP

FortiAuthenticator can dynamically look up G Suite and Azure group memberships for SAML SP FSSO.

Support for additional DC event log types

FortiAuthenticator can now parse Windows security event IDs 4769, 4770, 673 to update the active SSO sessions list. In addition, when DC event log polling is enabled (*Fortinet SSO Methods* > *SSO* > *General*), you can specify which event IDs to use in event log polling.

Export intermediate CA certificate and private key

You can export the certificate and private key of intermediate Certificate Authorities from the Local CAs page (*Certificate Management* > *Certificate Authorities* > *Local CAs*). This is useful in situations where you want to use the FortiAuthenticator as a Certificate Authority.

Support for Microsoft Azure and Oracle Cloud deployments

FortiAuthenticator VM now supports deployment on Microsoft Azure and Oracle Cloud.

Upgrade FortiAuthenticator firmware through CLI

The following CLI command has been added to perform firmware upgrades via FTP/TFTP:

```
execute restore image tftp <filename string> <tftp server>
execute restore image ftp <filename string> <ftp server>
[:port] [ftp_user] [ftp_password]
```

Upgrade instructions

Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator configuration, see the FortiAuthenticator Administration Guide.

Hardware and VM support

FortiAuthenticator 6.0.0 supports:

- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000C
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, and Azure)

Deprecated hardware models

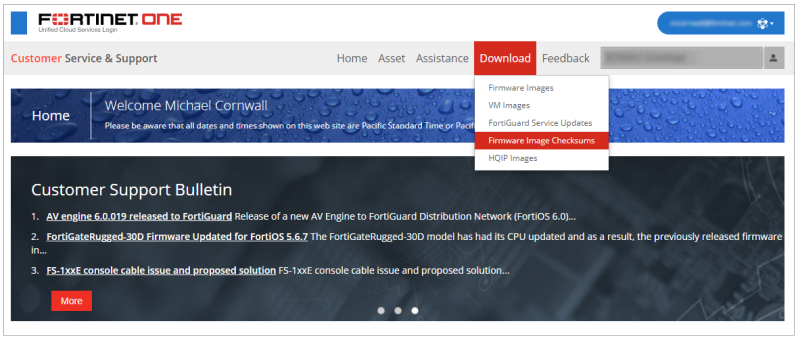
FortiAuthenticator 1000C has reached its End of Support (EOS) date. FortiAuthenticator 6.0.0 will be the last supported release for this model.

Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from the Fortinet Support website.

Customer service and support image checksum tool



After logging in to the web site, in the menus at the top of the page, click **Download**, then click **Firmware Image Checksums**.

In the **Image File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Upgrading from FortiAuthenticator 4.x/5.x

FortiAuthenticator 6.0.0 build 0010 officially supports upgrade from all versions of FortiAuthenticator 4.x.x and 5.x.x, with the exception of 5.3.1.

Upgrading FortiAuthenticator from 5.3.1 to 6.0.0 is not supported. The workaround for this is to upgrade from 5.3.1 to 5.5.0 first before upgrading to 6.0.0.

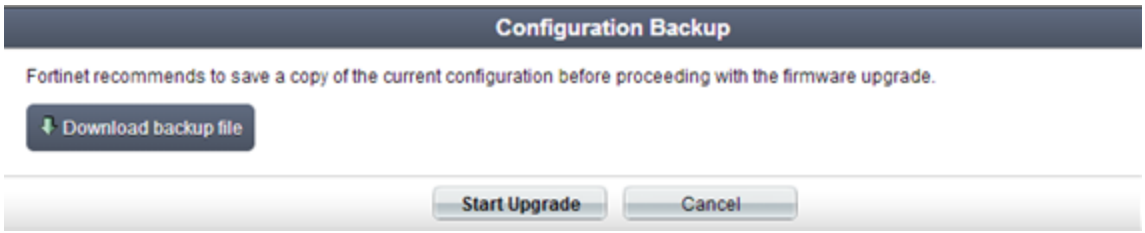
Firmware upgrade process

First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator firmware, you must download the firmware package from the Fortinet Support website, then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the Fortinet Support website. In the **Download** section of the page, select the **Firmware Images** link to download the firmware.
2. To verify the integrity of the download, go back to the **Download** section of the login page and click the **Firmware Image Checksums** link.
3. Log in to the FortiAuthenticator unit's web-based manager using the **admin** administrator account.
4. Go to **System > Dashboard > Status**.
5. In the **System Information** widget, in the **Firmware Version** row, select **Upgrade**. The **Firmware Upgrade or Downgrade** dialog box opens.
6. In the **Firmware** section, select **Choose File**, and locate the upgrade package that you downloaded.
7. Select **OK** to upload the file to the FortiAuthenticator.

Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:



It is recommended that a system backup is taken at this point. Once complete, click **Start Upgrade**.

Wait until the unpacking, upgrade, and reboot process completes (usually 3-5 minutes), then refresh the page.

Product integration and support

Web browser support

The following web browsers are supported by FortiAuthenticator 6.0.0:

- Microsoft Internet Explorer versions 9 to 11
- Microsoft Edge 42
- Mozilla Firefox versions 65
- Google Chrome versions 72

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAuthenticator 6.0.0 supports the following FortiOS versions:

- FortiOS v6.0.4
- FortiOS v5.6.8
- FortiOS v5.4.10
- FortiOS v6.2.0 Beta 3

The above versions have been verified by QA. Other FortiOS versions may function correctly, but may not be supported by Fortinet. Refer to the What's new section and Known issues for version compatibility information.

Fortinet agent support

FortiAuthenticator 6.0.0 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 2.2
- FortiAuthenticator Agent for Outlook Web Access 1.5
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but may not be supported by Fortinet.

For details of which operating systems are supported by each agent, please see the install guides provided with the software.

Virtualization software support

FortiAuthenticator 6.0.0 supports:

- VMware ESXi / ESX 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5
- Microsoft Hyper-V 2010, Hyper-V 2012 R2, and Hyper-V 2016
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine (for Xen HVM and AWS)
- Microsoft Azure

Support for HA in Active-Passive and Active-Active modes has not been confirmed on the FortiAuthenticator for Xen VM at the time of the release.

See FortiAuthenticator VM on page 16 for more information.

Third-party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor
- Token Passcode Appended - Supports any RADIUS compatible system

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS). For more information, see the FortiAuthenticator Two-Factor Authentication Interoperability Guide.

FortiAuthenticator VM

FortiAuthenticator VM system requirements

The following table provides a detailed summary on FortiAuthenticator virtual machine (VM) system requirements. Installing FortiAuthenticator VM requires that you have already installed a supported VM environment. For details, see the FortiAuthenticator VM Install Guide.

VM requirements

Virtual machine	Requirement
VM form factor	Open Virtualization Format (OVF)
Virtual CPUs supported (minimum / maximum)	1 / 64
Virtual NICs supported (minimum / maximum)	1 / 4
Storage support (minimum / maximum)	60 GB / 16 TB
Memory support (minimum / maximum)	2 GB / 1 TB
High Availability (HA) support	Yes

FortiAuthenticator VM sizing guidelines

The following table provides FortiAuthenticator virtual machine (VM) sizing guidelines based on typical usage. Actual requirements may vary based on usage patterns.

VM sizing guidelines

Users	Virtual CPUs	Memory	Storage
1 - 500	1	2 GB	1 TB
500 to 2,500	2	4 GB	1 TB
2,500 to 7,500	2	8 GB	2 TB
7,500 to 25,000	4	16 GB	2 TB
25,000 to 75,000	8	32 GB	4 TB

Users	Virtual CPUs	Memory	Storage
75,000 to 250,000	16	64 GB	4 TB
250,000 to 750,000	32	128 GB	8 TB
750,000 to 2,500,000	64	256 GB	16 TB
2,500,000 to 7,500,000	64	512 GB	16 TB

FortiAuthenticator VM firmware

Fortinet provides FortiAuthenticator VM firmware images in two formats:

- **.out**
  Use this image for new and upgrades to physical appliance installations. Upgrades to existing virtual machine installations are also distributed in this format.
- **ovf.zip**
  Use this image for new VM installations. It contains a deployable OVF virtual machine package for initial VMware ESXi installations.

For more information see the FortiAuthenticator product datasheet available on the Fortinet web site, https://www.fortinet.com/products/identity-access-management.html#models-specifications.

Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please visit the Fortinet Support website.

Bug ID	Description
527119	OCSP shows incorrect certificate status.
537510	Increase the VM_Base certificate table size.
537413	The DH parameters are not updated when upgrading firmware to version 5.4 or higher.
528680	Guest portals created from the migration of the legacy MAC address captive portal do not preserve the disclaimer setting.
526455	FortiToken Mobile transfer email message displays an incorrect expiration time.
526820	Push notifications aren't sent out to remote users when another user with the same username (but different realm) is present.
528211	SYSLOG SSO stops working after upgrade to firmware version 5.5.0.
529463	FortiAuthenticator randomly drops all FSSOMA sessions.
537945	Support multiple username attributes in FSSO LDAP user lookup when multiple remote LDAP servers in the same domain are configured.
517959	Duplicate DCs appear under domain in FSSO if FQDN is configured in LDAP.
526095	SAML authentication fails when signing the service provider request with a local certificate.
506294	FortiAuthenticator truncates SSO groups in long SAML attributes resulting in log on failures.
525263	SAML SP using Azure does not work.
535754	Username case sensitivity is removed from RADIUS authentication, but not from FSSO.
532689	FortiAuthenticator FSSO usernames containing spaces are ignored in event polling.
503366	Monitor SSO Domains shows a domain controller as red on HA Master and green on HA backup.
520572	When the pre-login disclaimer is enabled, the FSSO login widget requires two clicks instead of one.
527359	Unable to send randomly generated passwords via SMS when admin approval is required.

Bug ID	Description
532079	Guest Portal-triggered RADIUS authentication follow-up does not include group-name VSA in Access-Accept on first attempt.
535038	Radius group-name attribute is not sent to the FortiGate during initial authentication of social user causing authentication to fail.
532016	Unable to import SSO users with a DN longer than 255 characters.
509121	FSSO Logged-in users shows "N/A" in the User Inventory widget when there are users logged into the system.
538546	Error occurs when switching a local user from Sponsor to Admin.
534736	LDAP query fails if the query string contains non-ascii characters.
534347	Creating or importing Mac devices with names containing non-ascii characters causes a server crash.
532894	Registration is misspelled 'Registeration' on the self-registration page.
526637	When changing user type to admin, 'Allow Radius Auth' option should automatically be deselected.
519150	Spaces preceding and following the SAML IdP server address and service provider settings fields should automatically be removed.
512109	When setting up SAML IdP, selecting a third-party server certificate that is still in a pending state causes a server crash.
511667	The Change Password page does not have a Cancel button.
455084	The Debug Page for Radius Accounting crashes when displaying logs with non-utf-8 characters.
515429	An error can cause loss of access to the FortiAuthenticator GUI.
516167	An admin profile with "read-only" permissions for the SSO Monitor can log off authenticated users.
538016	Unable to assign a FortiToken to another user if the user has been already deleted on FortiAuthenticator.
504695	When exporting a guest user with the Print function, the resulting page includes unnecessary content.
521547	Mobile phone numbers with seven or eight digits do not work with SMS Gateway
540391	Finding "last backup" date/time can cause delays or failure of the System Information widget.
534879	Fix typo in error message when uploading an organization image.
521183	Rename Fortinet CAs.

Bug ID	Description
307386	FortiAuthenticator version upgrade history should be part of config backup/restore.
528440	The FortiAuthenticator GUI crashes after adding a guest portal rule.
522611	Rename "Meru" guest portal label to "Social portal pinholes".
523622	Coordinated HA upgrade produces two log entries under Upgrade History on the master.
522057	Deleting a social user on a LB slave will cause a crash to occur.
538865	FortiAuthenticator units fail to form a cluster when configuring HA active-passive mode.
534338	Factory reset / data drive formatting is extremely slow in Azure/HV/KVM.
526507	Remote user sync rules do not assign FortiToken to imported LDAP users.
524350	Tokens are not correctly assigned to local users during import rule execution.
490281	Column titled 'Type id' in the GUI logs is titled 'Log id' in the downloaded logs.
523780	Include Token Transfer Code in log entry.
520514	System reboots and shutdowns, intended or unintended, should be logged.
494705	Domain authentication fails for users from trusted domains due to missing domain name in authentication request.
530590	"Force password change on next logon" option does not work with FortiGate SSL-VPN if FortiToken Mobile push is used.
528580	FortiAuthenticator radiusd is unable to recognize client defined by hostname after DNS change.
493318	Remote LDAP users with expired passwords receive incorrect error messages when login fails.
526616	Auth REST API endpoint concatenated password+token_code in password field doesn't authenticate users.
519655	REST API: localusers endpoint accepts invalid parameters when sent via the PATCH method.
519652	Changing the FortiToken Mobile provisioning PIN length via REST API causes a server error.
400466	Support signed authentication requests with embedded signature for SAML IdP.
542547	SAML IdP user sessions expire earlier than configured session timeout.
539134	Typo in default replacement message for SAML Login Message Page.

Bug ID	Description
513278	Remote LDAP displayName attribute isn't included in SAML assertion for remote LDAP admin.
522350	Miscellaneous performance improvements to SAML authentication.
531734	SAML IdP: support special character '&' in SP URLs and multiple ACS URLs.
535136	SAML IdP needs to add "SessionIndex" inside "saml:AuthnStatement" on successful logins.
504081	SCEP requests from an iPhone fail due to an error "The SCEP server returned an invalid response.".
526242	UTF8STRING-encoded challengePassword within CSR sent during SCEP enrollment is not parsed correctly.
523340	Sending SMS messages using Twilio fails.
519994	When the sysOID is queried, FortiAuthenticator-VM identifies itself as a LINUX Net-SNMP agent system rather than a Fortinet device.
397184	Unable to monitor the FSSO user count via SNMP.
502007	The RADIUS accounting and CoA does not take effect on FortiAuthenticator.
464556	Time-based user expiry configured in usage profile isn't applied to users when they already have an expiry date configured.
485564	Fixed vulnerability to "TCP sequence number approximation based denial of service" attack.
411510	Fixed vulnerability to "Reverse Tabnabbing" attack.

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please visit the Fortinet Support website.

Bug ID	Description
540551	FortiAuthenticator should automatically recognize the configured IP address on ports other than port1 in Azure cloud.
540904	LB master should ratelimit its rechecks / changelog entries generated.
542734	SMS gateway on FortiAuthenticator is not delivering the token when used with RADIUS authentication.
537871	Unable to authenticate LDAP attribute rfc822MailMember on FortiAuthenticator-VM.
542808	CLI HA Status shows "Status: Error Status" on new build/factory reset FortiAuthenticator units.
415685	FortiToken-only users can log into a service provider configured to enforce two-factor authentication if the user already has an active session.
482900	User registration via Guest Portal requires the approver to enable radius authentication first.
541826	Assigning a profile to an admin user that restricts the 'Administrator' permission to read-only changes the user type to Sponsor.
532604	The Social Login Users list displays 'unknown' in the User column.
526202	FortiAuthenticator does not check if signature of CSR is valid.
530392	Cannot log in with social users on Guest Portal if their account has expired.
468513	Excluding a user from SSO causes FSSO server to exit and not recover.
536211	FortiAuthenticator should limit FSSO passwords to 15 characters since that is the limit on FortiGate.
524131	There is a multisecond delay between queuing and sending of push notifications
516358	SQL connections don't reliably timeout when underlying VPN tunnels time out.
541043	SAML authentication with Azure UUID mapping does not include SSO group for user as expected.
542094	SAML SSO cannot handle SAML assertion request: invalid information for passport-saml signature.
519319	FortiAuthenticator VM may crash when LDAP Remote user sync rules run.

Bug ID	Description
538244	Add option for SAML IdP to send Subject NameID in "example.com\username" format.
537628	For new deployments and after factory resets, FortiAuthenticator VM can experience a slow startup.
528231	The FortiAuthenticator log details state "cannot add any more users because limit has been reached".
538216	FortiAuthenticator FSSO service is unstable due to crashing DC agent daemon.
540932	FSSOMA nested group search fails if nested via primary group.
540933	Source IP is missing for authentication requests coming from FSSO Windows agent.
505897	Chained token authentication with remote RADIUS server breaks PCI.
540611	When user account gets locked because time/data usage is exceeded, FortiAuthenticator doesn't ask for a token, even if PCI is enabled.
540587	GUI crash occurs when clicking a guest user in an LB slave.
511093	In an HA setup, Radiusd on the LB slave crashes if a large custom RADIUS dictionary is uploaded to the master.
538059	Importing an ecdsa-signed certificate/key causes an error dump.
516357	Toggling load-balancing off and back on in an existing cluster can impact availability for hours/days.
537298	For Azure, NameID assertion in SAML should reference the username instead of the UserID.
506112	REST API call fails to activate FortiGuard Messaging license.
536029	Deactivate the option to disable secure passwords after 30 days have passed.
532652	Users Audit Report not working on Slave of LB cluster.

Maximum values for hardware appliances

This section lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware models.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

The following table describes the maximum values set for the various hardware models.

Feature		Model				
		200E	400E	1000D	2000E	3000E
System						
Network	Static Routes	50	50	50	50	50
Messages	SMTP Servers	20	20	20	20	20
	SMS Gateways	20	20	20	20	20
	SNMP Hosts	20	20	20	20	20
Administration	Syslog Servers	20	20	20	20	20
	User Uploaded Images	39	114	514	1014	2014
	Language Files	50	50	50	50	50
Realms		20	80	400	800	1600
Authentication						
General	Auth Clients (NAS)	166	666	3333	6666	13333
	Users (Local + Remote)[1]	500	2000	10000	20000	40000
	User Radius Attributes	1500	6000	30000	60000	120000
	User Groups	50	200	1000	2000	4000
	Group Radius Attributes	150	150	600	6000	12000
	FortiTokens	1000	4000	20000	40000	80000
	FortiToken Mobile Licenses[2]	200	200	200	200	200
	LDAP Entries	1000	4000	20000	40000	80000
	Device (MAC-based Auth.)	2500	10000	50000	100000	200000

Feature		Model				
		200E	400E	1000D	2000E	3000E
	RADIUS Client Profiles	500	2000	10000	20000	40000
	Remote LDAP Servers	20	80	400	800	1600
	Remote LDAP Users Sync Rule	50	200	1000	2000	4000
	Remote LDAP User Radius Attributes	1500	6000	30000	60000	120000
FSSO & Dynamic Policies						
FSSO	FSSO Users	500	2000	10000	20000	200000[3]
	FSSO Groups	250	1000	5000	10000	20000
	Domain Controllers	10	20	100	200	400
	RADIUS Accounting SSO Clients	166	666	3333	6666	13333
	FortiGate Services	50	200	1000	2000	4000
	FortiGate Group Filtering	250	1000	5000	10000	20000
	FSSO Tier Nodes	5	20	100	200	400
	IP Filtering Rules	250	1000	5000	10000	20000
Accounting Proxy	Sources	500	2000	10000	20000	40000
	Destinations	25	100	500	1000	2000
	Rulesets	25	100	500	1000	2000
Certificates						
User Certificates	User Certificates	2500	10000	50000	100000	200000
	Server Certificates	50	200	1000	2000	4000
Certificate Authorities	CA Certificates	10	10	50	50	50
	Trusted CA Certificates	200	200	200	200	200
	Certificate Revocation Lists	200	200	200	200	200
SCEP	Enrollment Requests	2500	10000	50000	100000	200000

[1] Note that **Users** is the only metric used for the number of allowed users. **Local Users** and **Remote Users** share the same limit value. This enables **Local Users** *or* **Remote Users** to be equal to **Users** or for there to be a mixture of user types, however, the total number of local and remote users cannot exceed the **Users** metric.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

[3] For the 3000E, the total number of concurrent SSO users is set to a higher level to cater for large deployments.

Maximum values for VM

This section lists the maximum number of configuration objects that can be added to the configuration database for different FortiAuthenticator virtual machine (VM) configurations.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

The FortiAuthenticator VM is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator VM Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The **Calculating metric** column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator VM Base License, the number of auth clients (NAS devices) that can authenticate to the system is:

100 / 10 = 10

Where this relative system is not used e.g. for static routes, the **Calculating metric** is denoted by a "**-**". The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

The following table describes the maximum values set for the various VM configurations.

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
System					
Network	Static Routes	2	50	50	50
Messaging	SMTP Servers	2	20	20	20
	SMS Gateways	2	20	20	20
	SNMP Hosts	2	20	20	20
Administration	Syslog Servers	2	20	20	20
	User Uploaded Images	19	Users / 20	19	250
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (NAS)	3	Users / 3	33	1666

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
User Management	**Users** (Local + Remote)[1]	5	**********	100	5000
	User RADIUS Attributes	15	Users x 3	300	15000
	User Groups	3	Users / 10	10	500
	Group RADIUS Attributes	9	User groups x 3	30	1500
	FortiTokens	10	Users x 2	200	10000
	FortiToken Mobile Licenses (Stacked) [2]	3	200	200	200
	LDAP Entries	20	Users x 2	200	10000
	Device (MAC-based Auth.)	5	Users x 5	500	25000
	RADIUS Client Profiles	3	Users	100	5000
	Remote LDAP Servers	4	Users / 25	4	200
	Remote LDAP Users Sync Rule	1	Users / 10	10	500
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
FSSO & Dynamic Policies					

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
FSSO	FSSO Users	5	Users	100	5000
	FSSO Groups	3	Users / 2	50	2500
	Domain Controllers	3	Users / 100 (min=10)	10	50
	RADIUS Accounting SSO Clients	10	Users	100	5000
	FortiGate Services	2	Users / 10	10	500
	FortiGate Group Filtering	30	Users / 2	50	2500
	FSSO Tier Nodes	3	Users /100 (min=5)	5	50
	IP Filtering Rules	30	Users / 2	50	2500
Accounting Proxy	Sources	3	Users	100	5000
	Destinations	3	Users / 20	5	250
	Rulesets	3	Users / 20	5	250
Certificates					
User Certificates	User Certificates	5	Users x 5	500	25000
	Server Certificates	2	Users / 10	10	500
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	5	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users x 5	2500	10000

[1] Note that there is one metric used for the number of allowed users which is **Users**. **Local Users** and **Remote Users** share the same limit value. This enables **Local Users** *or* **Remote Users** to be equal to **Users** or for there to be a mixture of user types, however, the total number of local and remote users cannot exceed the **Users** metric.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.